REMARKS

In this Response, Applicant amends claims 1, 4-6, 8-10, 17, 19, 28, 30, 33, 34, and 37 and removes the basis for the Examiner's rejections. Amendments to the claims are being made solely to expedite prosecution of the present application and do not constitute an acquiescence to any of the Examiner's rejections. Support for the amendments to the claims can be found throughout the application. Applicant reserves the option to further prosecute the same or similar claims in the present or a subsequent application. Upon entry of the Amendment, claims 1-11, 17-20, and 28-37 are pending in the present application.

Petition for Extension of Time

As provided in accompanying documents, Applicant petitions for a one-month extension of time under 37 C.F.R. § 1.136(a) in which to file this Response.

Claim Rejections

35 U.S.C. § 112, ¶ 2

The Examiner rejected claim 33 under 35 U.S.C. § 112, ¶ 2 as lacking antecedent basis for "said program code for publishing said certificate."

As provided herein, Applicant amends claim 33 to depend from claim 32, rather than claim 30. This amendment removes the basis for the Examiner's rejection.

35 U.S.C. § 103(a)

The Examiner rejected claims 1, 4, 5, 7-9, 11, 17, 18, 20, 34, 36, and 37 under 35 U.S.C. § 103(a) as being unpatentable over de Silva.

The Examiner also rejected claims 2, 3, 6, 10, 19, 28-33, and 35 under 35 U.S.C. § 103(a) as being unpatentable over de Silva in view of Vaeth.

Claims 1-11

Applicant's independent claim 1 is directed to a method for certificate generation. Among other things, Applicant's independent claim 1 includes a first node and a second node. The first node receives a request for issuing a certificate on behalf of a principal and forwards the request to the second node, in which the request includes a first identifier that identifies the first node. Subsequently, the second node generates a certificate that includes *the first identifier for the first node from whom the second node received the corresponding request for the certificate.*

Applicant agrees with the Examiner's statement that de Silva "does not explicitly state that the certificate includes said first identifier." Applicant also agrees with the Examiner's identification of an advantage to be gained from modifying de Silva's certificates to include Applicant's claimed *first identifier*, specifically, the advantage of "allow[ing] the system [to] more securely monitor[] the generated certificates." Since de Silva does not address the technical problem that is solved by Applicant's independent claim 1, though, Applicant respectfully requests that the Examiner reconsider the conclusion that she drew from that advantage, specifically, that those of ordinary skill in the art would have found it obvious to modify de Silva's certificates to include Applicant's claimed *first identifier* in light of the advantage to be gained.

In one embodiment, Applicant's independent claim 1 can be understood to relate to a scenario that includes a principal, a local registration authority "RA," and a central certificate authority "CA." In the scenario, the RA can receive a request from the principal for issuing the certificate. The RA can forward the request for the certificate to the CA and include in the request an identifier for the RA. Subsequently, the CA can issue the certificate and include in the certificate *the identifier for the RA from whom the CA received the corresponding request for the certificate.*

The integrity of the above RA-CA scenario can be compromised by compromising the RA. For example, if a hacker were to hack into the RA, the hacker could instruct the RA to send a request for a phony certificate to the CA. Since the CA issues certificates on request of the RA, the CA would issue the phony certificate to the RA. By compromising the RA, therefore, the hacker could acquire a phony certificate that would allow him to impersonate a principal.

Applicant's independent claim 1 provides a solution to the problem of a compromised RA in the RA-CA scenario. Specifically, in one embodiment, Applicant's independent claim 1 includes generating, at the CA, a certificate that includes *an identifier for the RA from whom the CA received the corresponding request for the certificate*. In one such embodiment, if the CA learns that an RA was compromised, the CA can revoke all certificates issued by the RA merely by publishing the identifier of the RA in a certificate revocation list.

de Silva does not address the problem of a compromised RA in an RA-CA scenario. Rather, de Silva merely describes an implementation of the RA-CA scenario in which the RA receives a request for a certificate from a principal and converts the request to a format specified by the CA. At most, de Silva states, without elaboration, that the CA can revoke a certificate of a principal. (See de Silva col. 5, ll. 1-2, stating merely "Revocation -- Central server 104 revokes client 102's digital certificate.") de Silva never teaches or suggests the possibility of a compromised RA, let alone Applicant's claimed method of addressing that possibility.

Since de Silva does not teach or suggest the feature of Applicant's independent claim 1 directed to a second node that can generate a certificate that includes *a first identifier*, i.e., *an identifier for the first node from whom the second node received the corresponding request for the certificate*, or the technical problem that is solved by that feature, those of ordinary skill in the art would not have found it obvious to modify de Silva's certificates to include Applicant's claimed *first identifier* and thereby obtain Applicant's independent claim 1.

Additionally, the advantage identified by the Examiner in modifying de Silva's certificates to include Applicant's claimed *first identifier* actually demonstrates that Applicant's invention is non-obvious. As the Examiner indicated, Applicant's invention enables a system to monitor generated certificates more securely. So prior workers in this art would have adopted it—and thereby availed themselves of its advantages—if doing so had been obvious. Since none did so, the conclusion properly to be drawn from the advantage is that the invention was not obvious.

Independent claim 1 therefore defines patentable subject matter. Since claims 2-11 depend from independent claim 1, they do, too.

Claims 17-20 and 28-37

Applicant's independent claims 17, 28, 30, and 34 are directed to certification authorities, computer program products, computer data signals, and apparatuses and include features similar to independent method claim 1. Applicant's independent claims 17, 28; 30, and 34 are therefore allowable for the reasons provided with respect to independent claim 1. Since claims 18-20, 29, 31-33, and 35-37 depend from independent claims 17, 28, 30, and 34, claims 18-20, 29, 31-33, and 35-37 are also allowable.

CONCLUSION

On the basis of the foregoing Amendment and Remarks, this application is in condition for allowance. Accordingly, Applicant requests allowance. Applicant invites the Examiner to contact the Applicant's undersigned Attorney if any issues are deemed to remain prior to allowance.

Respectfully submitted,
FOLEY HOAG LLP

Jeffrey M. Sears
Reg. No. 48,440
Attorney for the Applicant

Date: 2/25/2004

Customer No. 25,181
Patent Group
Foley Hoag LLP
155 Seaport Blvd.
Boston, MA 02210
Tel: (617) 832-3022
Fax: (617) 832-7000